06124467 **Image available**

EARLY DETECTING METHOD FOR ILLEGAL USE OF PASSWORD

PUB. NO.: 11-066004 [JP 11066004 A]
PUBLISHED: March 09, 1999 (19990309)
INVENTOR(s): TAKEDA HIDEO
APPLICANT(s): TAKEDA HIDEO
APPL. NO.: 09-249274 [JP 97249274]
FILED: August 12, 1997 (19970812)
INTL CLASS: G06F-015/00; G06F-001/00

ABSTRACT

PROBLEM TO BE SOLVED: To detect the illegal use of a password in an early stage at that time by issuing the new password from a center computer every time of communication.

SOLUTION: It is recognized whether an ID code is a registered one or not by the confirmation item (1) of the ID code at the beginning of communication. Then, the password is recognized by the confirmation item (2) of the password. Then, the new password is issued by the issuing item (3) of the new password. The reception of the password is confirmed and an original job is started by an original job item (4). The password is written by the issuing item of the password every time of communication. When the password is stolen and it is illegally used, the password is rewritten. Thus, when a just user is to use the password, the password is not matched and illegal use can be detected at an early stage.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－66004

(43)公開日　平成11年(1999)３月９日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ａ
	1/00	３７０		1/00	３７０Ｅ

審査請求　未請求　請求項の数１　書面　（全 3 頁）

(21)出願番号　特願平9－249274

(22)出願日　平成９年(1997)８月12日

(71)出願人　597131657
武田　英夫
東京都足立区宮城１－２－17

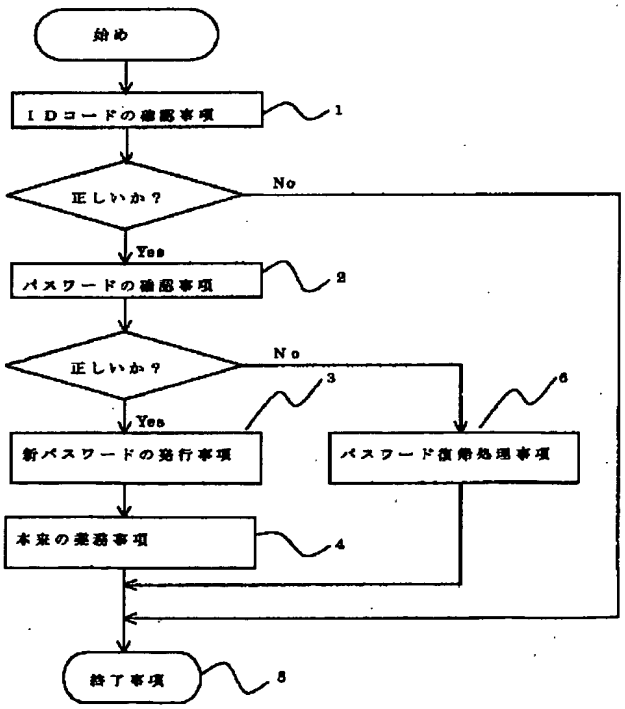
(72)発明者　武田　英夫
東京都足立区宮城１－２－17

(54)【発明の名称】　パスワード不正使用の早期発見方法

(57)【要約】

【課題】　コンピュータ通信におけるパスワードの不正使用を早期に発見し、早期に被害を食い止める。

【解決手段】　毎回通信するごとに、中央コンピュータから新しいパスワードを発行する。パスワードを盗まれ不正に使用されると、パスワードが書き換わる。そのため正当な使用者が次回通信したときにパスワードが合わなくなり、不正使用を早期に発見できる。パスワードは使用者側からは変更できないので、不当に使用した者が元のパスワードに戻そうとしても出来ない。



1

【特許請求の範囲】
【請求項１】　毎回通信するごとに中央コンピュータから新しいパスワードを発行する事を特徴とする、パスワード不正使用の早期発見方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、コンピュータ通信の不正使用防止に関するものである。
【０００２】
【従来の技術】正当な使用者である事を確認するためパスワードを使用しているが、パスワードを盗まれ不正に使用されても気付き難かった。従来の方法は次の通り。
（イ）使用者が定期的にパスワードを変更する。
（ロ）前回の通信終了時刻を知らせ、使用者がその時刻の通信が正当であったか判断する。
【０００３】
【発明が解決しようとする課題】従来の技術には次のような欠点が有った。
イ．パスワードの不正使用を常に点検しているのは手間が掛かる。
ロ．そのためパスワードを盗まれ不正に使用されても、被害が表面化するまで気付き難かった。本発明はパスワードが不正に使用されたとき、その事実を早期に発見するものである。
【０００４】
【課題を解決するための手段】毎回通信するごとに、中央コンピュータから新しいパスワードを発行する。パスワードを盗まれ不正に使用されると、パスワードが書き換わる。そのため正当な使用者が次回通信したときにパスワードが合わなくなり、不正使用を早期に発見できる。パスワードは使用者側からは変更できないので、不当に使用した者が元のパスワードに戻そうとしても出来ない。
【０００５】
【発明の実施の形態】ＩＤコードの確認事項（１）、パスワードの確認事項（２）、本来の業務事項（４）については、従来と同じである。本発明は、新パスワードの発行事項（３）である。
（イ）通信の初めにＩＤコードの確認事項（１）により、登録されたＩＤコードであるか確認する。正しくないときは、終了事項（５）に進み処理を終了する。
（ロ）パスワードの確認事項（２）により、パスワードを確認する。正しくないときは、パスワード復帰処理事項（６）に進む。
（ハ）新パスワードの発行事項（３）により、新しいパスワードを発行する。
（ニ）パスワードの受領を確認する。
（ホ）本来の業務事項（４）により、本来の業務に入る。
【０００６】このようにすると、毎回通信するごとに新

2

パスワードの発行事項（３）によってパスワードが毎回書き換わる。パスワードを盗まれ不正に使用された場合も、パスワードが書き換わる。そのため正当な使用者が使おうとしたときにパスワードが合わなくなり、不正使用を早期に発見できる。パスワードが不正に使用された時は、正当な使用者も使用できなくなる。そのための復帰処理が、パスワード復帰処理事項（６）である。なお、パスワードは端末側からは変更できない。そのため不正に使用した者が元のパスワードに戻そうとしても出来ない。
【０００７】パスワード復帰処理事項（６）の復帰処理の例を示す。
（イ）中央コンピュータに正当な使用者の電話番号を登録しておく。使用者が複数の端末から通信するのであれば、この電話番号は複数個でもよい。登録した電話番号の中から一つを指定して中央コンピュータから電話をしてもらう手続きをし、終了事項（５）に進んで通信を終了する。中央コンピュータからの電話を待ち、再度ＩＤコードの確認事項（１）から始める。この場合、パスワード確認事項（２）の処理は行わない。ＩＤコードは他人にも知られているので、パスワード復帰処理事項（６）の処理には、誰にも行くことが出来る。そのため電話番号を直接表示すると情報が漏れるので、「自宅」「事務所」などとしておく。パスワードを不正に使用した者によって、この電話番号が本来の業務事項（４）の中で変更されてはならない。そのためこの電話番号は本来の業務事項（４）の中で変更出来ないように、他の手段によって登録する。このままでは、中央コンピュータから無用な電話を掛けさせるという悪戯も出来る。それには、この対策のために他に用意した従来方式のパスワードを使えば対処できる。そのパスワードが破られても、中央コンピュータからの電話回数を制限したり、次の（ロ）の処理で回避できる。
（ロ）中央コンピュータ管理者に連絡し、復帰してもらう。
【０００８】パスワードが毎回変わるので、使用者もそれに対応した使い方が必要になる。使用者側の対応の例を挙げる。
（イ）　使用者以外が端末に触れない場合
パスワードの受領と確認はソフトウェアで自動に行い、パスワードは端末内に保管しておく。
（ロ）　端末に複数の人が触れるため、パスワードを盗まれる恐れがあるとき
上の（イ）でパスワードを端末内に保管せず、持ち運べる記憶媒体に保管する。
（ハ）　使用者が複数の端末を操作する場合
上の（ロ）に準じパスワードを記録した媒体を持ち運び、最新のパスワードをその端末に使う。
（ニ）　使用者側でソフトウェアを用意出来ないとき
背後からモニタ画面を見てパスワードを盗まれないよう

に、パスワードは表示しないのが普通である。それで中央コンピュータから送られてくるパスワードを表示するように設定し、使用者がそれを記録しておく。

【０００９】

【発明の効果】パスワードが不正に使用されたとき早期に発見し、早期に被害を食い止める。

【図面の簡単な説明】

【図１】本発明のフローチャートである。

【符号の説明】

１　登録されたＩＤコードであるか確認する

２　ＩＤコードに対応したパスワードであるか確認する。

３　新しいパスワードを発行し、受領したか確認する。

４　本来の業務

５　通信を終了する

６　パスワードが不正に使用されたとき、正当な使用者が使用できるように復帰処理

【図１】